ACROSS THE WORLD

It's a quiet evening in India. You're sitting with your laptop and decide to text your friend in Germany. You type, **"Hey, how are you?"** and hit **Send**.

At that very moment, something magical happens behind the scenes — your tiny packet begins its journey.

Scene 1: The Birth of a Packet

Your chat app takes your message and turns it into digital form — just a bunch of bytes that computers can understand.
But the problem is: your computer knows your friend's name as **friend.chatserver.com**, not his real address on the internet.

So it asks the **DNS resolver** — "Hey, what's the IP address of friend.chatserver.com?"

The resolver goes on a quick hunt through the DNS hierarchy — first the root servers, then the `.com` servers, and finally the chat app's own name servers. It comes back with an answer: **122.22.12.32**

Now your computer finally knows where to send your message.

Scene 2: The Handshake

(The alternative of TCP is UDP(User Datagram Protocol, which is faster than TCP but less reliable, Hence we stick with TCP and the entire set of protocols is called TCP/IP)

Before sending the message, your computer makes sure there's a reliable path. It starts a TCP handshake — a short digital greeting:

- You send **SYN** →
- The server replies **SYN-ACK** →
- You respond **ACK**

Done! The connection is ready — a tiny "nice to meet you" between your device and the server in Germany.

Scene 3: Leaving Home

Your packet gets an **IP address** — your home IP as the source and your friend's server IP as the destination. {IP address are assigned to ensure each IP packet can reach the correct destination}

But since you're using Wi-Fi, your router with **NAT** replaces the private IPs with one shared public IP when sending data to the Internet, then with a quick signal, your packet travels through your Wi-Fi, enters your router, and zooms into the network of your Indian ISP.

Scene 4: Inside the ISP

Now your packet is moving inside your Internet Service Provider's network.
Powerful routers guide it step by step, using maps called **OSPF** or **IS-IS** to find the shortest path.

It passes through fibre cables and network switches until it reaches the **international gateway** — the point from where it will leave India.

Scene 5: The Undersea Adventure

Next stop: the ocean.

Your packet dives into an **undersea fibre-optic cable**, carrying data at almost the speed of light.

They carry your message into Europe — all guided by **BGP (Border Gateway Protocol)**, which helps big networks talk to each other and decide the best route.

Scene 6: Arrival in Europe

After just a few milliseconds, your packet reaches Europe.
Routers in Germany pick it up and pass it through local networks until it finally reaches your friend's home Wi-Fi router.

There, it gets translated back from the public Internet into his home network — and lands safely on his laptop.

Scene 7: Message Delivered

His computer puts all the tiny TCP pieces back together in the right order.
The chat app unwraps it and shows your message:
"Hey, how are you?"

Your packet has done its job perfectly.

Scene 8: The Return Journey

Your friend types back, **"I'm good!"**

His packet now begins the same trip in reverse — but it might take a slightly different path, because BGP routes can change.
It could pass through France or even Singapore this time, but every router knows how to get it back to you.

Your home router uses its NAT table to remember which connection belongs to which device — so it delivers the reply right to your laptop.

Scene 9: Internet Traffic Jams

Sometimes, the network gets busy.
Routers may get overloaded, and packets might be delayed or lost.

If your packet disappears on the way, **TCP** automatically notices and resends it — kind of like resending a text when the signal's weak.

That's how the Internet controls its "traffic."

Scene 10: Security and Privacy

If you were chatting over **HTTPS**, your app and the server first did a **TLS handshake**, where they exchanged encryption keys.
That means even if someone tried to spy on the undersea cable, all they'd see would be scrambled code — useless gibberish.

The server's digital certificate also proves it's real and not a fake.

Scene 11: The Hidden Hero — DNS

Without **DNS**, none of this would work.
It's the Internet's phonebook — converting website names into IP addresses.
It quietly did its job before your packet even left India, and its answer guided the whole journey.

Scene 12: Back Home

Your friend's reply travels all the way back — through routers, across continents — until it reaches your ISP in India.

Your router checks its list, recognizes the connection, and hands it to your computer.

Your chat app finally shows **"I'm good!"** on your screen.

All this happens in less than a second.

Epilogue

So your little "Hey" wasn't just a message — it was an **adventure**.
It met routers, traveled through fibre cables, crossed oceans, followed protocols like **TCP/IP** and **BGP**, and still came home safe.

Every time you send a message, remember — there's a whole world of technology working quietly behind the scenes, making sure your words reach the right person, almost at the speed of light.

NOTE TO SELF

List of protocols in the application layer,

DNS - IP<->Domain name

DHCP - Auto assigns IP address

FTP - Transfer files

HTTP - sends & receive webpages

IMAP - E-mail messages

IRC - Internet chat

POP3 - Retrieve messages

SMTP - Email messages

NAT - Network Address Translation - It is a process your router allows multiple devices use the same internet connection

IP (Internet Protocol) - IP is what moves packets from one place to another, every computer has an IP Address, it handles what path to take (Routing) and who sends the message to whom (Addressing), it doesn't look at the data

TCP (Transmission Control Protocol) - makes sure your data arrives safely without any loss. It does a 3-way handshake SYN → SYN-ACK → ACK

BGP (Border Gateway Protocol) - choose the right pathway between networks across continents (global)

5 Layers of TCP/IP protocol suite

- Application Layer

  when browser uses DNS to find the IP address of the website, eg. HTTP, etc

- Transport Layer

makes sure there is an end to end connection and data arrives and delivers safely without any loss, eg. TCP, UDP,etc

- Internet Layer

decides the best route for internet packet to go from my device to the website i opened on my browser, eg. IP, ARP

- Network Access Layer

once the route is known, it gives us access to the medium through how it data packets will move, eg. WiFi, DSL

- Physical Layer

data now moves as electric signals, aka bits